Best Practices for DeltaV Cyber-Security

This document describes best practices will help you maintain a cyber-secure DeltaV digital automation system.

Table of Contents

Introduction

Keeping a DeltaV system secure from hacker attacks, viruses, worms and other malware and security threats requires that everybody who deals with the system follow an established set of system security best practices. The best practices listed in this document can be treated as requirements or as simple guidelines for keeping a system secure. It is up to each organization – customer or integrator – to set the proper security policies for their particular organizations or to meet the needs of a specific situation.

This document is supplementary and complimentary to the “DeltaV System Cyber-Security” whitepaper. See this whitepaper for more background on cyber-security issues and the DeltaV system.

For the purposes of this best practices document, and in line with generally accepted terminology, “cyber-security” includes all non-physical threats to the network. This includes hacker penetration of the network, any deliberate or accidental access by an unauthorized user and the introduction of viruses, worms or other malware intended to disrupt the activities of the network or to access confidential information. To avoid unnecessary repetitions, the term “attack” will include virus, worms, malware, Trojans and other automated intrusion-enabling software, as well as direct manually directed attacks by persons outside the control network.

Procedures and User Training—System Security Policies

In addition to the best practices involving the use of technology solutions and physical security, having good security procedures and proper user training are important to establishing and maintaining system cyber-security. Each section in this document may include some recommendations for user training to complement the technically oriented best practices.

A key element to defense in depth (aka Rings of Protection) is having developed a security policy. System cyber-security is all about risk management. The security configurations we design, the OS and application patches we install, the firewalls and intrusion detection applications we implement – all come down to risk management.

Effective network security is dependent on a workable, communicated security policy. A security policy will document the threats (risks) to your system, which threats you are willing to accept, and which ones you have to mitigate. Only by having a security policy can you decide which threats must be accepted or mitigated. After you have that policy in place, you can start appropriately applying these best practices to your system.

A security policy will also bring to light the risks that can best be solved using technology and which can only be done by procedures and training to educate users about threats and how to avoid being attacked.

The use of this best practices document assumes that you have some level of security policy available to determine how and if each of these guidelines would be used in your facility.

Overall System Cyber-Security

Our overall system security is based on three elements:

Physical Access – physical isolation of the control equipment in locked rooms or cabinets to prevent unauthorized access to equipment

User Access – authentication and authorization – the proper implementation of user password security and role-based access control to prevent unauthorized access on DeltaV user terminals within the plant

Network Isolation – network isolation of the DeltaV Control Network from the plant LAN and any other LANs with “open access.”

System Design Practices

The DeltaV system must be kept isolated from the plant LAN.

- Follow the DeltaV procedures for the network configuration where all connections to the plant LAN must be made through a DeltaV workstation. See Figure 1.
- Network connections to the plant LAN should not be made unless absolutely necessary to run the process, maintain the system or for valid business reasons.
- Ensure that there are no other networks, modems or wireless connections designed into the network except for the necessary connections as determined in item 2 above.
- Any modem that might have been installed for remote technical support should be identified and made secure or removed from use. If the modem is required, it should be set up to act in a call-back mode and should require user password access at the modem interface once the call back is made. A procedure for unplugging the modem between uses is not recommended, as it leaves the system open to access if the user forgets to unplug the device.

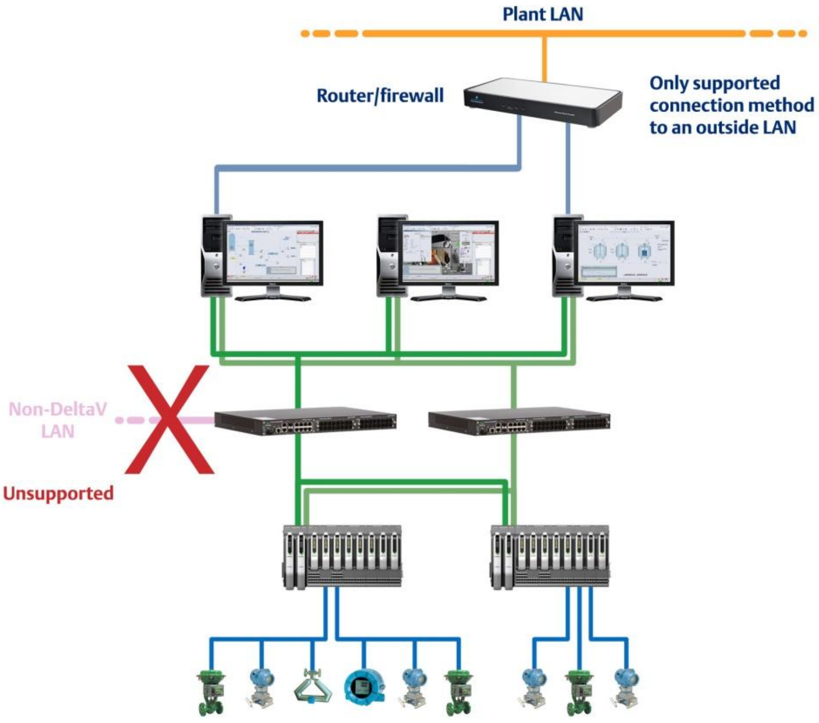

Figure 1 - DeltaV LAN architecture keeps the system isolated from the plant LAN.

System Configuration and Integration Practices

Organizations involved in the configuration and integration of a DeltaV system have a responsibility to maintain a secure environment for the DeltaV system. Viruses, worms and malware can attack a system from any network connection. It is possible to stealth install unwanted and undesirable software at any time. Maintaining a secure system is important even during system integration. This section of best practices is specific to handling a system while it is in the integration process, regardless of the location where actual tasks are being done.

When a PC is received from Dell and prior to any external network connections being made, the following should be done:

- The latest supported security patches from Microsoft should be installed.
- The latest supported Symantec anti-virus program and the latest anti-virus signature files should be installed.
- The anti-virus program and anti-virus signatures must be kept up-to-date at all times.

A DeltaV Operator Station should be configured to disable the Internet browser application from making connections to the internet. A workstation user must never be able to open the Internet Explorer and connect to an external internet site.

E-mail programs must never be run on any DeltaV workstation or any computer directly connected to the DeltaV LAN at any time.

During DeltaV installation, all default user passwords should be changed to prevent unauthorized users from accessing the system. Only the personnel actually engineering the system should know the passwords for that specific system. Accounts should be set up consistent with the duties of each user. Administrator privileges should be reserved for only the very few individuals who will be responsible for these tasks – in general, users who are performing engineering tasks

The DeltaV system should never be connected to any network unless it is properly protected with a correctly configured firewall. The firewall should specifically block any/all port 80 traffic (Internet) and any port that could be used for e-mail traffic. All ports should be blocked in both directions except for those needed for the applications on the DeltaV network.

Each person doing configuration work on the DeltaV system should have a unique account (user-specific name and password), so user activities can be properly controlled.

All user accounts not required for commissioning and startup should be deleted from the DeltaV system before the system is shipped to the customer. After startup is complete, all non-customer accounts should be deleted. To insure only authorized customer accounts remain on the system after implementation the customer administrator should change the admin password and delete any vendor accounts.

At this time, if a vendor account is required, the user should set this up with the proper user keys. But it is strongly suggested that these accounts be given limited capabilities and disabled until actually needed. These vendor accounts should be enabled only for the time required for the vendor to provide the necessary service and then disabled again.

General business laptop or desktop computers should never be used as DeltaV workstations, nor should they ever be connected into the DeltaV system. Data should be moved between general purpose laptops and desktops by the use of USB thumb drives or CDs. All portable media must be virus scanned prior to insertion into a DeltaV workstation.

If you find a virus-infected computer during integration, an anti-virus program may not completely clean it. Since other undetectable malicious programs may have also been installed, it is a best practice that computers that become infected should have the hard drive reformatted and the system completely reinstalled. This is done to ensure no traces of the infection remain and to remove any undetected malware.

The intention of these practices is to ensure that the customer receives the most cyber-protected, cyber-secure system possible. An integrator must be able to verify that they have kept the customer system in a secure environment at all times.

DeltaV Security Best Practices: A Quick Overview

Basic system security for a DeltaV system is relatively easy to implement and monitor:

Physical Security

- Computers and network devices should be mounted in secure cabinet.
- Control rooms should be secure.
- Open, logged-on workstations should not be left unattended without locking down the desktop

Anti-virus security

- Install and maintain anti-virus software per DeltaV instructions.
- Disable access to the floppy and CD-ROM drives.
- Disable access to unused USB ports, especially those on the PC front panel. (This may require physically disconnecting the ports within the computer).

Password Security

- Properly maintain user lists – add required users only and delete unneeded users immediately.
- Do not use shared user names and passwords.
- Change all default passwords immediately upon system install.

Network Security

- All plant LAN connections to the DeltaV system must be made through a workstation.
- Routers and firewalls must be used to isolate this connection from the plant LAN.
- Block all network ports except those required for DeltaV connections.
- Limit users that can connect by IP address, MAC address or other criteria.
- All users must have their own user name and password.
- Limit access to only those who can justify access.
- Utilize data access vs. system access to keep data only users off the actual system.
- Use a dual firewall protection scheme for optimum protection.

- For high security applications, install intrusion detection and monitor logs periodically.

DeltaV Security Details

The sections below provide more details on DeltaV system security. The information is presented in a sequential format where securing the system in a stand-alone implementation is the foundation before further securing the system as network access is added to the environment.

Securing a Stand-alone DeltaV System

Even when a system is isolated and not connected to other communications systems, there are security risks that must be considered. Securing physical access and local user access to the system becomes the primary security action.

- Maintain Passwords
- No email or web access
- Disable CD-ROM and diskette drive
- Disable USB ports
- Do not leave remote units available
- Secure in locked cabinets if possible

Figure 2 - Lock down workstations to prevent unauthorized access

The first-level and primary system security is based on limited physical access to the DeltaV workstations, network equipment and controllers and I/O. We expect that as necessary to ensure a secure control system the user has a secure plant location with controlled access to the physical plant and the control room and process area where the system(s) are located.

Within these areas good security practice dictates:

- Controllers and network equipment should be installed in locked or sealed enclosures that prevent easy access by unauthorized personnel. Network switches should have unused network ports disabled. This is to prevent an internal access by unplugging a network device for access or simply plugging into an unused port on a network device.

- Even if computers are physically secured in locked cabinets, the floppy and CD drives should be disabled or unplugged to prevent users from introducing viruses and other malware programs into the system.

- Even in an enclosure, it is possible for maintenance personnel to introduce problems if they use untested CD or floppy media for troubleshooting tasks. Any such software needs to be protected, and there should be procedures for properly verifying that this software remains virus free.

- USB ports (except those actually in use for keyboards, mice or peripheral devices) should be physically disconnected so they cannot be accessed by unauthorized users.

- Network cable runs, especially in remote areas, should also be protected from easy access.

Access to the control room where operator consoles are available should also be controlled – at least to the extent that the personnel in the room are policing the access to the workstations.

Operators should not leave open console access while a control room is unattended. Consoles should always be locked out while they are unattended.

On remote located console, operating procedures should dictate that operators log out or lock consoles when not in use. At a minimum, consoles should be set up so they automatically lock the screen after a very short time of inactivity: no more than a 2-minute delay is recommended.

Any computers or other smart devices connected to the DeltaV network for maintenance purposes should have processes in place to ensure that the devices are certified free of virus and malware before they are connected.

In addition, authorization should be required for plant personnel and visitors to carry laptop computers or other portable devices with network connections (including Ethernet wireless access) into the process plant. Unauthorized access can be made and systems can be infected with malware from network connections made to non-secure portable equipment.

To aid plant personnel in identifying and reporting unauthorized devices it is suggested that any authorized devices be easily identifiable (painted a conspicuous color or labeled in some visible manner) so unauthorized equipment is easily identified.

To protect against unauthorized wireless access points being connected to the system, areas where network equipment is installed should be periodically scanned for wireless signals, using inexpensive wireless signal monitoring devices.

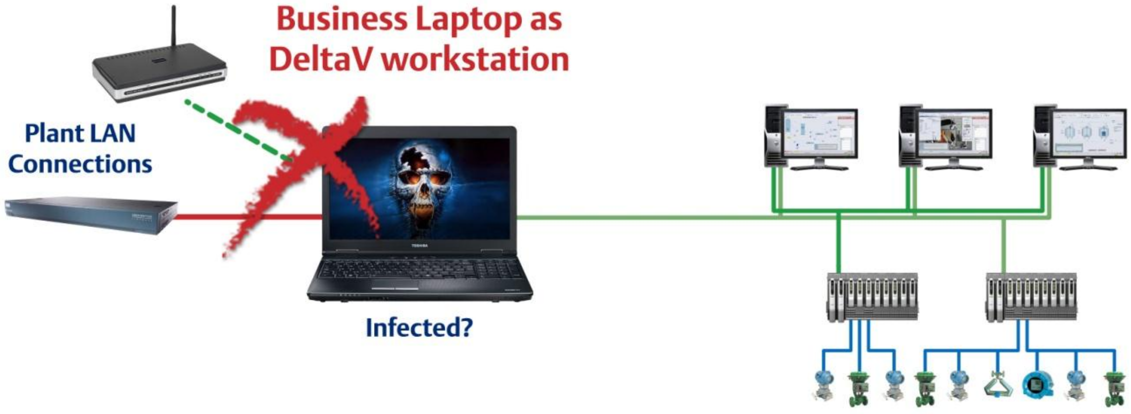

Figure 3 - Laptops can be a source of malware and unauthorized network connections

If laptops are used as DeltaV workstations (not a DeltaV supported solution):

- They should be dedicated for DeltaV functions and never connected to an “open” LAN.
- To maintain the system isolation, laptops that are also used as general purpose business computers (with Internet access and e-mail) should never be used as DeltaV workstations directly connected to the DeltaV LAN.

User Access—Password Security

After physical access security, the next level of securing the DeltaV system is to control user access via a password protection scheme. DeltaV password access is multi-level and provides two levels of security, plus the ability to set up role-based security privileges for each user. Each user with authorized access to a DeltaV system must have both a Microsoft user account and a DeltaV user account.

Passwords must be properly maintained to prevent unauthorized access from people gaining physical access to the system:

- Default passwords must be reset.
- Proper roles must be assigned to each user.
- User access must be carefully maintained.
- Users who no longer need access must be removed.
- Users without significant business reasons should not be given access.
- A system access and password policy should be in place and enforced.
- Generic or shared user names and passwords should not be used.

Microsoft’s OS provides security configurations that allow each user (or groups of users) to have specific Microsoft privileges for desktop access (such as access to run, delete or modify files) to prevent unauthorized users from access to files, programs, and information on the workstation. Within the DeltaV system, it is up to the individual user administrators to correctly set up these security features to prevent access or to provide the correct level of access for each user. It is up to the user to set up the proper user privileges for file and application access.

If control changes are required on a running process as part of system development implementation, good practice would dictate that these changes be made by a qualified operator under the instruction of a known supervisor, rather than by the supervisor acting alone.

In any case, operators should never provide their personal user names or passwords to others including engineers or supervisors. Plants concerned about security should not use generic user names or passwords for any users. Each user should have a personal, private logon setup.

A user with authorized access to the workstation, but who is not a DeltaV user, cannot access the DeltaV software and functions. So it is possible to grant administrative access to the system without providing any access to DeltaV functions

Role-based Security Access

The DeltaV system also provides role-based security. Each user must be specifically granted privileges to gain access to DeltaV applications. Operators can be given plant-wide authorization, or their span of control can be limited by plant area to access only specific functions based on their job duties or roles within the plant. Engineers can be given just configuration privileges but not download or operate capabilities. To maintain system security, it is up to the customer facility to train operators and other users on the proper rules for using and updating their passwords.

Virus Prevention and Detection

As a best practice, Emerson Process Management recommends that, at a minimum, anti-virus software must be installed on any workstation connected to an outside LAN. For additional protection, anti-virus software should be installed on every workstation on the DeltaV network. Emerson Process Management supports the current versions of Symantec (Norton) Anti-Virus. There is a separate whitepaper on this topic called “Symantec Anti-Virus and DeltaV” that covers the specific aspects of deploying the anti-virus software on the DeltaV system. See this whitepaper for details.

Approved Software for DeltaV Workstations

Security can also be impacted by the installation of non-approved software on a DeltaV workstation. Non-approved software in this case is any software that has not been approved by the customer’s DeltaV system administrator to be installed on the workstations. As a best practice, only a very limited number of system support personnel should have administrator privileges for loading software and other admin tasks. DeltaV does not require a logged in user to have system administration privileges to configure, operate, or download a DeltaV system.

Securing a Connected DeltaV System

Once the user makes a network connection to an outside system, additional aspects of security must be considered. These security procedures are in addition to those mentioned above in the section “Securing a Stand-alone DeltaV System.”

All network connections between a DeltaV system and a plant or other outside LAN must be made through a DeltaV workstation protected by a router/firewall. Direct connections between an outside LAN and DeltaV network hubs or switches are not permitted or supported. See the next section, “Protecting the Network Interface to a DeltaV System” for details on this connection.

DeltaV connections use specific ports for communications, and all other ports not used for DeltaV applications should be closed or disabled to prevent connections being made through other open ports. In the event other ports are required for customer-installed software, then only those ports should be allowed open. Details of firewall configuration are provided in separate documents.

All connections to DeltaV applications require some level of user authentication (even the DeltaV WebServer). Since only specific persons with permissions to connect will be allowed access to the system, the setup of the firewall/router should be made to allow only those specific individuals or computers to connect to the system. This setup can easily be tightened down to prevent unauthorized access because the DeltaV connections should not be set up for general access.

All connections from the outside into the DeltaV system must be set up with user-specific passwords. Security is easily compromised if a generic user name/password is distributed for access.

Most companies or sites have some sort of password policies and, at a minimum; these should be followed for control system users as well. We suggest a strong password policy be adopted to prevent easy cracking of passwords. Password changing should also follow corporate guidelines or be set up on a 90-day rotation. Default passwords should not be used and must be changed during implementation of the system.

It is important that the DeltaV system administrator keep control of the user setup for DeltaV users. They should know who and why a person is granted access. Access should be tightly controlled and users who no longer need access (such as contractors who are used only during initial implementation or employees who change responsibilities or leave the company) should be removed immediately.

Under no circumstances should a DeltaV workstation run an e-mail application or make a general-purpose, open-use connection to the Internet. The connection firewall should block all port 80 outbound connections or email port connections. If it is required for operators to access e-mail or the Internet, then separate plant network computers not connected to the DeltaV LAN should be used for these applications.

Protecting the Network Interface to a DeltaV System

At a minimum, the connection between a workstation node on a DeltaV LAN and an external LAN (regardless of whether or not DeltaV is installed on the node) must be protected by a router/firewall device. The firewall should be set up as required to allow only specific users to access the system and to block access through any ports not specifically needed to support the DeltaV connections to the outside LAN. Specifically, port 80 for the Internet and all ports that would allow e-mail access must be closed or blocked.

Maintaining access through a workstation creates an interface called a demilitarized zone (DMZ) which creates a buffer zone between the DeltaV LAN and the external LAN. In this configuration, the workstation acts as a "neutral zone" between control network and the plant network. It prevents plant users from getting direct access to the devices on the control network. Isolating the network from the plant LAN greatly reduces the opportunities for unauthorized access from outside the plant or from users of the plant LAN who should not be accessing the control network.

Note that when using a firewall, change management procedures to prevent unauthorized or improper changes that would compromise security of proper data flow should be developed and followed.

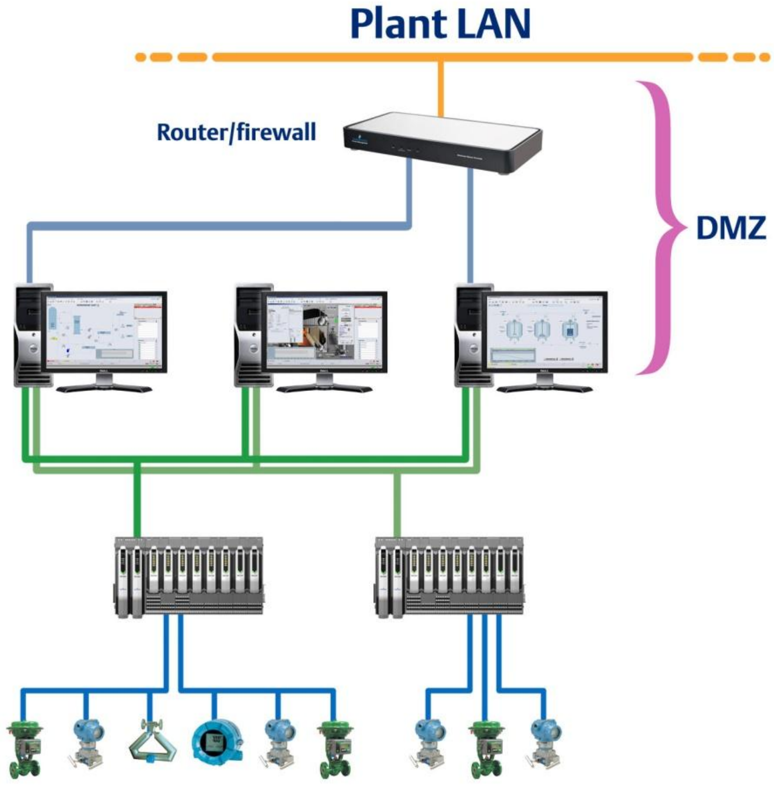

Figure 4 – All network connections must be made through a workstation and protected by a firewall

Using Two Firewalls for Optimum Security

The preferred solution for providing a higher security system is to use two router/firewalls and create a secure interposing “process LAN” between the control system and the plant LAN. See the figure below for a picture of this setup. For optimum security, it is suggested that two firewalls from different vendors should be used. This provides an attacker more difficulty in getting to the control LAN, even if they are successful in getting through the firewall from the plant LAN because they would have to learn to hack another firewall type. It is also suggested that access through the control system firewall be managed by operations or the process control/DeltaV administrator to ensure that the proper permissions have been granted to any individuals getting system access to the DeltaV workstations.

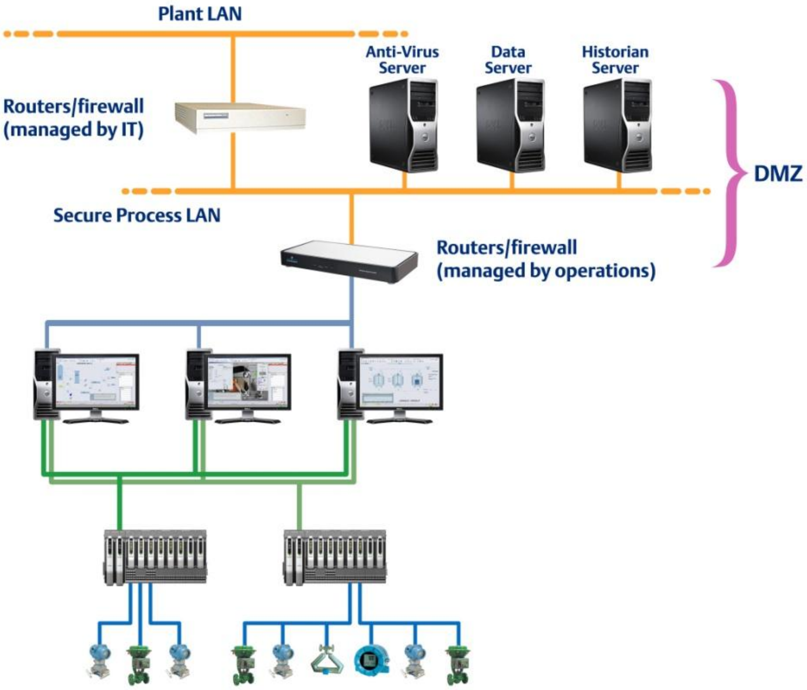

Figure 5 - Dual firewalls provide a more secure system than a single firewall.

Data Access vs. System Access

This dual router/secure process LAN arrangement promotes system security based on the concept of data access vs. system access. Most remote users require only data access to view plant operating data or to help with process troubleshooting. It is not necessary to provide these users with access to the actual control system nodes because access to data is sufficient for their requirements.

Process data access is provided for users on the plant LAN from the data and historian servers. The DeltaV system provides the process data to these servers on a real-time or on an as-needed basis so the plant LAN users who need only data access never connect to a node on the control system. For clarity, the functions are shown on separate servers on the LAN, but these functions could be combined in a single computer on the LAN. However, since users can be easily segregated to specific computers, it is often more secured to install these functions on the separate computers so that users can be allowed access only to the specific functions/data that they need.

The anti-virus server shown on the process LAN is used to hold and distribute the updated virus signatures to the DeltaV workstations. Virus data is supplied to this server from a secure node on the plant LAN or manually from CDs. This also allows the control system administrator to manage the distribution of the DAT files to the control system nodes.

Remote users who need access for engineering functions or administrative tasks can be given system access to workstations on the DeltaV LAN using DeltaV RAS or DeltaV Remote Client. Since remote access for these functions is typically limited to a specific and finite set of users, it becomes much easier to configure the firewall into the control system LAN to allow access only from these individuals either by hardware MAC address or static IP address and client node name.

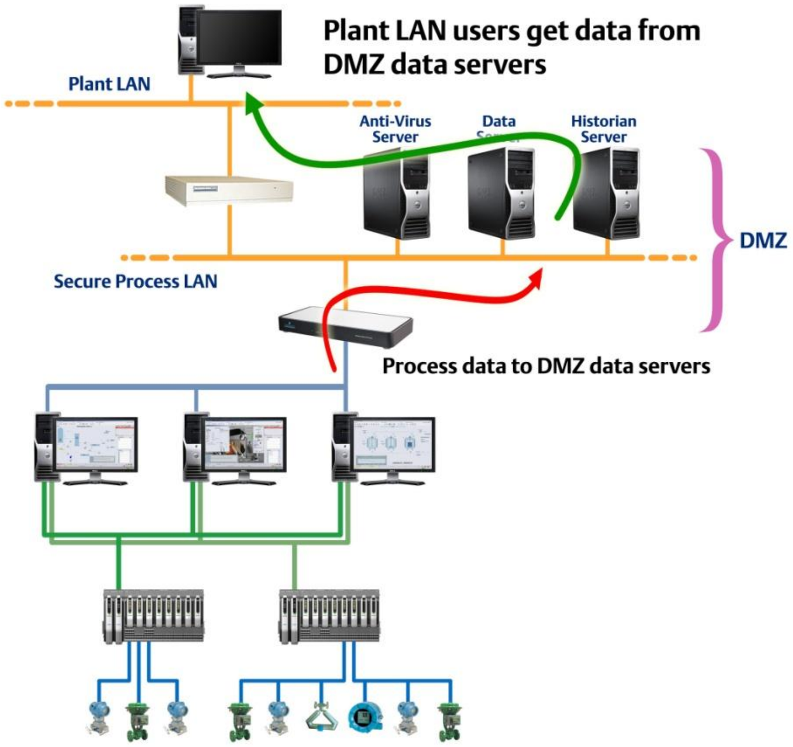
Plant LAN users get data from DMZ data servers
Plant LAN
Anti-Virus Server
Data
Historian Server
DMZ
Secure Process LAN
Process data to DMZ data servers

Figure 6 - Accessing data from the DMZ servers helps control unnecessary access to the control system.

Intrusion Detection

Network intrusion detection systems (NIDS), monitor packets on the network wire and attempts to discover if a hacker is attempting to break into a system (or cause a denial of service attack). A typical example is a system that watches for large numbers of TCP connection requests to many different ports on a target machine, thus discovering if someone is attempting a TCP port scan. A NIDS may run either on the target machine that watches its own traffic (not supported on a DeltaV workstation), or on an independent machine promiscuously watching all network traffic (preferred DeltaV solution). A "network" IDS monitors many machines, whereas the others monitor only a single machine (the ones on which they are installed).

In most networks, the NIDS is located at the firewalled connection from the Internet to the corporate or plant LAN. This way, intruders can be detected before they get onto the internal LANs. Also the NIDS requires IT resources to monitor the communication logs for abnormal activity, which adds costs to this solution. Depending on the control system security risk analysis done by the user, the cost of using a NIDS between the plant and control LANs can be justified.

If a NIDS is used as part of a DeltaV system protection solution, it should be installed between the plant LAN and the plant LAN router/firewall. NIDS logs require analysis to detect attack/intrusion patterns, and this activity is usually best left to the experts in the IT organization rather than the operations department.

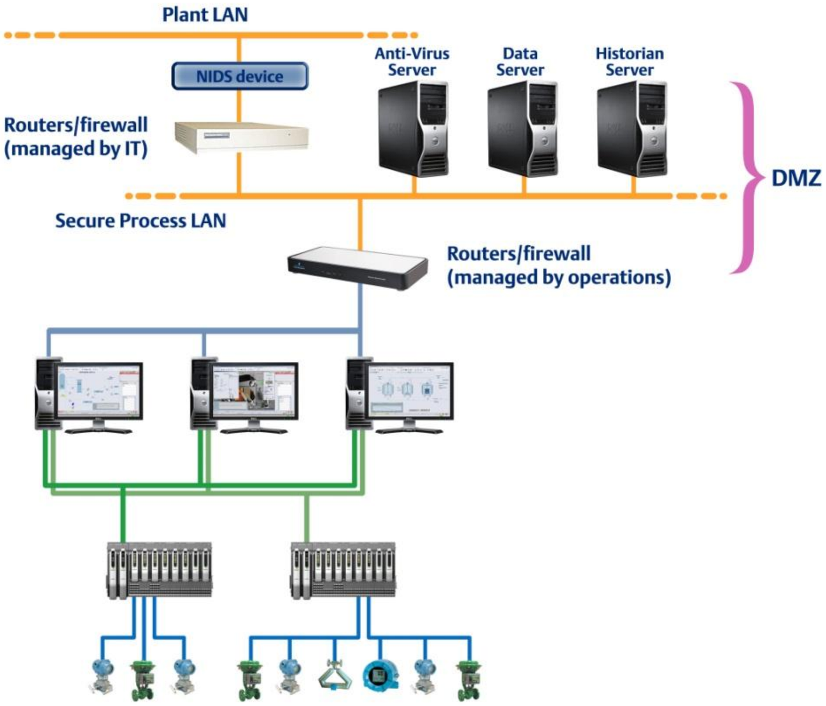

Figure 7 - A NIDS can provide additional security for a DeltaV system.

Summary

Performing a system risk assessment and then implementing the appropriate security practices outlined in this whitepaper will allow the user to provide adequate and cost-effective security for the DeltaV automation system. If further help is required with site-specific DeltaV security, implementation personnel in our SureService group can be contracted to provide this service.

This page intentionally left blank.

To locate a sales office near you, visit our website at:
www.EmersonProcess.com/DeltaV
Or call us at:
Asia Pacific: 65.6777.8211
Europe, Middle East: 41.41.768.6111
North America, Latin America: +1 800.833.8314 or
+1 512.832.3774

For large power, water, and wastewater applications contact Power and Water Solutions at:
www.EmersonProcess-powerwater.com
Or call us at:
Asia Pacific: 65.6777.8211
Europe, Middle East, Africa: 48.22.630.2443
North America, Latin America: +1 412.963.4000

© Emerson Process Management 2013. All rights reserved. For Emerson Process Management trademarks and service marks, go to: http://www.emersonprocess.com/home/news/resources/marks.pdf.

The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warrantees or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the design or specification of such products at any time without notice.